May 23, 2002

Information System Security

Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System
(D-2002-093)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Report Date	Report Type	Dates Covered (from... to)
23 May 2002	N/A	-

Title and Subtitle Information System Security: Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System	**Contract Number**
	Grant Number
	Program Element Number
Author(s)	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD(ATTN: AFTS Audit Suggestions) Inspector General Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Report Number** D-2002-093
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Sponsor/Monitor's Acronym(s)**
	Sponsor/Monitor's Report Number(s)

Distribution/Availability Statement
Approved for public release, distribution unlimited

Supplementary Notes

Abstract
Public Law 106-398, Government Information Security Reform, title X, subtitle G of the Floyd D. Spence National Defense Authorization Act for FY 2001, October 30, 2000, requires that each agency obtain an independent assessment of its security posture. The Inspector General of each agency is required to evaluate the agencys security posture based on a review of an independently selected subset of information systems. The DoD uses information technology for thousands of processes that are integral to support and operational functions. Mission-critical, mission-essential, and support-function processes, or applications, reside on computer systems throughout DoD. DoD selected a sample of 560 automated information systems from the almost 4,000 automated information systems in DoD. For those 560 systems, DoD developed a Government Information Security Reform Act collection matrix that was used to gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices. DoD reported the aggregate results of the assessments for FY 2001 in GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense, October 2001. Of the 560 systems, the Office of the Inspector General of the Department of Defense; the Defense Information Systems Agency Inspector General; and Military Department Audit Agencies assessed a sample of 115 systems. This report is one in a series of Government Information Security Reform Act audits and is an assessment of the Noncombatant Evacuation Operations Tracking System.

Subject Terms

Report Classification unclassified	**Classification of this page** unclassified

Classification of Abstract unclassified	**Limitation of Abstract** UU
Number of Pages 29	

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General of the Department of Defense Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DMDC	Defense Manpower Data Center
GISR	Government Information Security Reform
NTS	Noncombatant Evacuation Operations Tracking System
SSAA	System Security Authorization Agreement

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202–4704

May 23, 2002

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE (COMMAND, CONTROL, COMMUNICATIONS, AND INTELLIGENCE)
DIRECTOR, DOD HUMAN RESOURCES ACTIVITY

SUBJECT: Audit of the Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System (Report No. D-2002-093)

We are providing this report for information and use. This audit was conducted in accordance with the provisions of the Government Information Security Reform Act, title X, subtitle G of the Floyd D. Spence National Defense Authorization Act for FY 2001, October 30, 2000 (Public Law 106-398).

Because this report contained no recommendations, no written response to this report was required, and none was received. Therefore, we are publishing this report in final form.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Mr. Tilghman A. Schraden at (703) 604-9186 (DSN 664-9186) (tschraden@dodig.osd.mil) or Ms. Kathryn L. Palmer at (703) 604-8840 (DSN 664-8840) (kpalmer@dodig.osd.mil). See Appendix C for the report distribution. Audit team members are listed inside the back cover.

Thomas F. Gimble
Acting
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2002-093 **May 23, 2002**
(Project No. D2002LD-0069)

Government Information Security Reform Act Implementation: Noncombatant Evacuation Operations Tracking System

Executive Summary

Introduction. Public Law 106-398, "Government Information Security Reform," title X, subtitle G of the Floyd D. Spence National Defense Authorization Act for FY 2001, October 30, 2000, requires that each agency obtain an independent assessment of its security posture. The Inspector General of each agency is required to evaluate the agency's security posture based on a review of an independently selected subset of information systems.

The DoD uses information technology for thousands of processes that are integral to support and operational functions. Mission-critical, mission-essential, and support-function processes, or applications, reside on computer systems throughout DoD.

DoD selected a sample of 560 automated information systems from the almost 4,000 automated information systems in DoD. For those 560 systems, DoD developed a Government Information Security Reform Act collection matrix that was used to gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices. DoD reported the aggregate results of the assessments for FY 2001 in "GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense," October 2001. Of the 560 systems, the Office of the Inspector General of the Department of Defense; the Defense Information Systems Agency Inspector General; and Military Department Audit Agencies assessed a sample of 115 systems. This report is one in a series of Government Information Security Reform Act audits and is an assessment of the Noncombatant Evacuation Operations Tracking System.

Results. In our assessment of the Noncombatant Evacuation Operations Tracking System, the Defense Manpower Data Center implementation of the Government Information Security Reform Act requirements, as reported in the Government Information Security Reform Act collection matrix for FY 2001, was generally accurate as of August 1, 2001, the date of the FY 2001 collection matrix data. Although 6 of the 32 responses provided in the collection matrix were technically inaccurate because the supporting documents were in draft form, we concluded that the Defense Manpower Data Center was making progress toward achieving full information security accreditation for the Noncombatant Evacuation Operations Tracking System by August 2002, the target date for completion of the FY 2002 collection matrix. For details on the audit results, see the Finding section.

Management Comments. We provided a draft of this report on May 3, 2002. Because this report contained no recommendations, written comments were not required, and none was received. Therefore, we are publishing this report in final form.

Table of Contents

Background

Government Information Security Reform. On October 30, 2000, the President signed the Floyd D. Spence National Defense Authorization Act for FY 2001 (Public Law 106-398), which includes title X, subtitle G, the "Government Information Security Reform" (GISR) Act. Subtitle G directs that the Government ensure effective controls for highly networked Federal information resources; management and oversight of information security risks; and a mechanism for reporting improved information system security oversight and assurance for Federal information security programs. The GISR Act directs each Federal agency (DoD for purposes of this report) to annually evaluate its information security program and practices and, as part of the budget process, submit the results of the evaluation to the Office of Management and Budget. The GISR Act covers both unclassified and national information security systems and creates a comparable security management framework for each. The GISR Act also requires that the agency Inspector General or other independent agent evaluate the agency information security program and practices. Also, the GISR Act requires each agency Inspector General or other independent agency to select and test a subset of systems that will confirm the effectiveness of the information security programs.

DoD Responsibilities. The GISR Act directs DoD to annually evaluate its information security program and practices. The DoD uses information technology for thousands of processes that are integral to support and operational functions. Mission-critical, mission-essential, and support-function processes, or applications, reside on computer systems throughout DoD. Applications for the DoD Components include financial accounting; personnel; pay and disbursement; materiel shipping, receiving, and storing; munitions maintenance; and weapon systems-associated applications.

The GISR Act directs that DoD as part of the budget process submit the results of their annual evaluation to the Office of Management and Budget. Office of Management and Budget guidance, memorandum 01-24, "Reporting on the Government Information Security Reform Act," June 22, 2001, directs the Secretary of Defense to transmit the FY 2001 annual evaluation of information security program and practices to the Office of Management and Budget by October 1, 2001. The Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) [ASD(C^3I)] formed and chaired an Integrated Process Team to develop and finalize the guidance and methodology for DoD reporting of the GISR Act. The Integrated Process Team developed a 32-column spreadsheet--GISR Act collection matrix--to gather data on assessments of the effectiveness of DoD information assurance policies, procedures, and practices. DoD required the FY 2001 GISR Act collection matrix data completion as of August 1, 2001.

Inspector General Responsibilities. Office of Management and Budget issued memorandum 01-08, "Guidance on Implementing the Government Information Security Reform Act," in January 2001 to provide implementation instructions for Federal agencies in carrying out the GISR Act. Guidance specific to the duties of each Inspector General as an independent evaluator was also included in that memorandum. The Office of Management and Budget guidance states

that each Inspector General or independent evaluator "should perform an annual evaluation of the agency's security program and practices. This testing includes testing the effectiveness of security controls for an appropriate subset of agency systems." Although the GISR Act applies to all Government information systems, Office of Management and Budget acknowledged that agencies could not review all of those systems every year. As a result, the independent evaluation should identify and assess a logical representative sampling of systems that can be used to form the basis of a conclusion regarding the effectiveness of an agency's overall security program.

DoD Systems. The Office of the Inspector General of the Department of Defense developed a stratified random sample from the population of automated information systems the DoD evaluated and reported for FY 2001 in the "GISR Report FY01: Government Information Security Reform Act, Report of the Department of Defense," October 2001 (DoD GISR Act Report). DoD selected and reported in the DoD GISR Act Report on a sample of 560 automated information systems from the almost 4,000 systems listed in the DoD Information Technology Registry.[1] The Office of the Inspector General of the Department of Defense stratified random sample included 115 systems from the universe of 560 systems that were reported on in the DoD GISR Act Report. The audit agencies for the Military Departments and the Defense Information Systems Agency, Inspector General will evaluate 91 of the information systems included in the sample 115 by August 2, 2002. The Office of the Inspector General of the Department of Defense will evaluate the remaining 24 systems that support DoD agencies and activities. This report discusses the evaluation of 1 of the 24 DoD-level systems, the Noncombatant Evacuation Operations Tracking System (NTS).

DoD Information Security Program. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process, (DITSCAP)," December 30, 1997, provides the procedures for certification and accreditation of information technology to include information systems, networks, and sites in DoD. It also assigns responsibilities for oversight and implementation of the certification and accreditation process. DITSCAP is to be used as guidance throughout the certification and accreditation process. DoD Manual 8510.1-M, "Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP) Application Manual," July 2000, provides implementation guidance that standardizes the certification and accreditation process throughout DoD.

[1]The Information Technology Registry was established in response to requirements contained in section 8102(a) of the National Defense Appropriation Act for FY 2001 and section 811(a) of the National Defense Authorization Act for FY 2001. The DoD registry must contain all of the fielded mission critical and mission essential systems as well as all the mission critical and mission essential systems that are in development.

Objectives

Our overall audit objective was to assess NTS for implementation of the GISR requirements of the Floyd D. Spence National Defense Authorization Act for FY 2001. See Appendix A for a discussion of the audit scope and methodology.

Noncombatant Evacuation Operations Tracking System Information Security

Data reported for NTS in support of the implementation of the GISR Act requirements for FY 2001 were generally accurate as of August 1, 2001. Of the 32 responses provided on the matrix, 6 were technically inaccurate because the supporting documents were in draft form. However, the Defense Manpower Data Center (DMDC)[2] was following DITSCAP to certify and accredit NTS. As a result, DMDC is making progress in achieving full information security accreditation for NTS by August 2002.

System Background

NTS is a mission essential[3] system developed to support noncombatant evacuation operations. Noncombatant evacuation operations are conducted during times of endangerment or as part of a military exercise to evacuate civilian noncombatants and nonessential military personnel from foreign or host nations. The purpose of the NTS is to provide individual accountability for noncombatant evacuees by creating and maintaining an automated database of evacuees assembled during an evacuation operation. NTS was initially developed in October 1998 for U.S. Forces Korea. Since that time, NTS has been deployed to the European (June 2000) and Pacific (February 2001) theaters of military operations.

Hardware Configuration. NTS is a set of commercial-off-the-shelf laptop computer workstations, scanners, miniservers, and main database server. Under normal operation, NTS is a stand-alone system (not required to be connected to a computer network to operate) that is not employed until evacuations or military exercises are conducted. When NTS is employed, the system is activated and a database is created.

System Operations. During an evacuation, evacuees report to an evacuation control center where information about the individual is gathered and entered in the system at an NTS registration workstation. The registration workstation (laptop computer) is capable of reading and processing a variety of scanned identification documents, including passports and DoD identification cards. Each individual is assigned a unique NTS tracking number that is linked to the individual's identification document. The tracking number is located on an identification bracelet similar to those hospitals use and must be worn by the evacuees. The data from the laptops used in the registration are saved to an evacuation control center miniserver by way of a wireless modem. Registered evacuees may include service members, DoD and non-DoD civilian employees; U.S. residents abroad, foreign nationals, corporate employees; and any dependents and pets.

[2]DMDC is the program office for NTS and is responsible for the continued development and maintenance of the system. DMDC is a component of the DoD Human Resource Activity.

[3]Mission essential systems are those systems that are basic and necessary for the accomplishment of an organization's mission.

Registration data from the miniservers are stored on a database server at the theater command level. The evacuation database server is a fully dedicated server that is not used for other automated systems. The evacuation database is saved to a DMDC server located at DMDC-West, Monterey, California, through a data extraction that DMDC initiates. DMDC can then post the evacuation database on the Web to provide access to Pentagon decisionmakers and planners. The status of an evacuee at each stage of the evacuation process is updated through scanning of the identification bracelet and can be provided on an official use only basis through a secure Web site. Access to the Web site must be cleared through DMDC.

Data Collection Matrix

DMDC through the DoD Human Resource Activity provided the response for the NTS to ASD(C^3I) as of August 1, 2001, and the data reported were generally accurate. In response to the GISR Act requirement for each Federal agency to annually evaluate and report on its information security program and practices, ASD(C^3I) developed a GISR Act data collection matrix (the matrix) for DoD. The Assistant Secretary developed the matrix as a management tool to track information assurance trends and outcomes. The matrix consisted of a spreadsheet divided into four sections for data. Section titles included identifying information, accreditation information, assessment criteria information, and operations and assessment interest items.

In response to the information in the matrix, DMDC was generally required to answer yes, no, or provide a date for action completed. With the exception of a special section that could be used for augmenting comments, no other explanation was required or expected. A discussion of each section of the matrix and the data that DMDC reported in the matrix for NTS follow, along with our analyses of the reported data for DMDC. Appendix B contains the information for NTS that was reported in the matrix that ASD(C^3I) used for the DoD GISR Act Report.

Identifying Information. DMDC was requested to provide the system/network name, acronym, component owner, and information technology classification (mission critical or mission essential) in the identifying information section of the matrix. DMDC responded in the matrix that NTS was under the component ownership of the DoD Human Resource Activity and was classified as a mission essential information technology system. We verified that the identification information in the matrix was essentially correct as stated in the DoD Information Technology Registry.

Accreditation Information. DMDC was requested to provide the date of accreditation certification, date of interim certification, the accreditation method, and documentation for certification and accreditation in the accreditation information section of the matrix.

Accreditation Date. DMDC was requested to provide the date that an accreditation process accredited NTS. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, establishes the minimum security requirements for DoD automated information systems. DITSCAP implements the Directive, assigns responsibility, and prescribes procedures for certification and accreditation. DMDC responded in the matrix by leaving the field blank. We verified that the lack of a DMDC response was appropriate. DMDC did not place a date in the field because NTS was in the process of applying DITSCAP requirements.

Interim Certification Date. DMDC was requested to provide the date that an interim authority to operate was granted. According to the provisions of DITSCAP, interim authority should be based on the establishment of an acceptable level of risk in operating the system. DMDC responded in the matrix that an interim authority to operate was granted to NTS on July 27, 2001. We verified that an interim authority to operate for 1 year was granted by the NTS Designated Approving Authority, the Director of DMDC, and that DMDC planned to complete the NTS certification and accreditation process prior to the expiration of the interim authority to operate.

Accreditation Method. DMDC was requested to identify if NTS was accredited under DITSCAP. Several policies govern actions of program officials, but DITSCAP is the principal governing document for risk assessment and mitigation of DoD information technology systems. DITSCAP establishes the oversight mechanism that ensures identification of appropriate information to certify, accredit, and maintain a program's security. DMDC responded in the matrix that they were using DITSCAP to certify and accredit the NTS. We verified that the NTS was following DITSCAP procedures, but DMDC should have responded "no" to the question because as of August 1, 2001, NTS was not accredited.

Certification and Accreditation Documentation. DMDC was requested to identify if formal documentation existed that the Inspector General of the Department of Defense or other entities could use to verify accreditation. DITSCAP requires a System Security Authorization Agreement (SSAA) for each information technology system. The SSAA is a formal and binding document among the system program manager, the Designated Approving Authority, the Certifying Authority, and the user representative that establishes the level of security required. The SSAA guides the process and documents the results for certification and accreditation as well as implementation of information technology security requirements. DMDC responded in the matrix that they had formal documentation in effect for the NTS certification and accreditation process. We confirmed that DMDC documented the NTS certification and accreditation process with a draft SSAA. However, as of August 1, 2001, the SSAA was in draft form and not a formal (signed) document. Therefore, DMDC should have answered "no" in response to having formal certification and accreditation documentation. DMDC planned to finalize the SSAA by August 2002, when the NTS is accredited.

Assessment Criteria Information. DMDC was requested to confirm that information assurance controls and plans in the assessment criteria information section of the matrix existed. According to the instructions provided for the matrix, ASD(C^3I) developed the assessment criteria information section to assess selected systems on the basic program management, controls, and procedures that exist as part of the operation of the system.

Access Controls. DMDC was requested to identify if access controls were in place. ASD(C^3I) defined access controls as controls that limited access of information system resources to authorized users, programs, processes, or other systems. DMDC responded in the matrix that access controls were in place. We verified that DMDC had access controls in place. Those access controls that NTS used included: users were required to identify themselves during system login through the use of a protected mechanism (such as passwords) to authenticate user identity and user accounts; and access to the authentication security accounts database and logon programs were denied to the NTS user.

Risk Assessment and Management Plan. DMDC was requested to identify if a risk assessment and management plan was completed. ASD(C^3I) defined risk as the possibility of something adverse happening; risk assessment as the process of analyzing threats and vulnerabilities of an information system, and the potential impact of lost information; and risk management as the process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk. DMDC responded in the matrix that a risk assessment and management plan was not completed. We verified that when DMDC submitted the matrix data as of August 1, 2001, they had not developed an NTS risk assessment and management plan. However, since that time, DMDC developed a draft NTS risk assessment and management plan. DMDC planned to finalize the risk assessment and management plan by August 2002.

System Life-Cycle Plan. DMDC was requested to identify if a system life-cycle plan existed. System life-cycle plan guidance that ASD(C^3I) provided with the matrix was that many models for the system life cycle exist but most contain five basic phases: initiation, development and acquisition, implementation, operation, and disposal. DMDC responded in the matrix that NTS had a system life-cycle plan. We confirmed that as of August 1, 2001, DMDC had a draft NTS life-cycle plan. Because the plan was a draft document that would not be finalized until the NTS is accredited, DMDC should have answered "no." During our review, NTS was in the implementation phase of DITSCAP compliance and was undergoing continuing development and upgrades. According to the draft life-cycle plan, short term (within 5 years) hardware upgrades were based upon whether the commercial-off-the-shelf equipment such as computers, passport readers, printers, and scanners met the system use criteria and were less expensive, smaller, and more structurally sound and rugged. Application software was to be updated annually, or as required, based on feedback from system users.

System Security Plan. DMDC was requested to identify if a system security plan was in place. ASD(C^3I) defined a system security plan as an overview of the security requirements of a system, a description of the controls in place or the controls planned for meeting those requirements, and delineation of responsibilities and expected behavior of the individuals who access the system. DMDC responded in the matrix that NTS had a system security plan.

We verified that DMDC had a draft system security plan for NTS as of August 1, 2001. DMDC should have responded "no" because the plan was a draft document that would not be finalized until NTS is accredited. The NTS draft system security plan was titled, "NTS Security Standard Operating Procedures Plan." The draft plan identified the security measures that must be enforced to operate the NTS so it can securely process sensitive unclassified information. In addition, the draft plan provided guidelines to assist personnel responsible for NTS security in directing the safeguarding of sensitive unclassified information contained in NTS equipment from unauthorized access and use, alteration, destruction, and denial of service. The draft plan also described the responsibilities of information system security personnel responsible for NTS, defined the requirements to maintain compliance with the accreditation, including periodic security reviews, risk management, a continuity of operations plan, required actions in the event of compromise, initial and periodic security training programs, and reaccreditation. Further, the draft plan prescribed detailed procedures the NTS site managers, administrators, and users were required to carry out that will ensure secure operation of the NTS. The security guideline procedures applied to all NTS operating sites.

Personnel Security Measures. DMDC was requested to identify if proper personnel security measures were in place. ASD(C^3I) defined personnel security measures as a broad range of security issues related to how human users, designers, implementers, and managers of software and hardware interact with computers, and the access and authorities needed to do their jobs. DMDC responded in the matrix that NTS had personnel security measures in place. We confirmed that personnel security measures were in place for NTS. NTS registrars' (operator and user) access and authority were limited to individuals required to perform and manage noncombatant evacuation operations. The noncombatant evacuation operation system administrators and evacuation control centers' officer in charge were responsible for authorizing operators and users. NTS users and operators had authorized access to only the information required to perform assigned tasks. The concept of "need to know" was primarily implemented in NTS systems through the use of password protection and physical access procedures. The NTS program officer at DMDC was responsible for controlling access to the NTS Web site.

Physical Security Controls. DMDC was requested to identify if physical security controls were in place. ASD(C^3I) defined physical security and environment security as the measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. DMDC responded in the matrix that NTS had physical security controls in place. We verified that physical security controls were in place at DMDC-West. Although the NTS plan for physical security includes physical security procedures for operational units that use the system, as a practical matter we did not verify the controls of the operational units in Korea, Japan, and Europe. Physical security controls for NTS included: equipment must be physically secure at all times, system components must be locked and secured when not in use, and when in use, access to the systems was limited to authorized users only. Additionally, the NTS was to be operated in facilities and areas that maintained physical security measures that comply with applicable Federal, Service-level, and local security policies.

Administrative Controls. DMDC was requested to identify if administrative controls were in place. ASD(C^3I) did not define administrative controls but suggested that administrative controls included the presence of a help desk and audit trail. Administrative controls are designed to promote operational efficiency and adherence to system policies and procedures. DMDC responded in the matrix that NTS had administrative controls in place. We verified the DMDC response. According to the NTS draft SSAA, user administrators (site designated approving authority, the site security officer, and Component-level system administrator) were responsible for ensuring that Federal, DoD, and local computer security-related standards were enforced. Even though no specific NTS system level administrative requirements were required, DMDC did staff an NTS help desk during noncombatant evacuation operation exercises.

Contingency Plans. DMDC was requested to identify if contingency plans were in place, and if so, when the last time was that a contingency drill, data loss, or power loss drill occurred. ASD(C^3I) defined contingency planning as involving more than simply planning for a move offsite after a disaster destroys a facility. Contingency planning was to also include how to keep an organization's critical functions operational in the event of disruptions, both large and small. DoD Directive 5200.28 requires periodic testing of contingency plans for mission critical systems and encourages contingency plans for all systems. DMDC responded in the matrix that NTS had contingency plans in place, but left the date the contingency plans were last exercised blank. We verified that NTS had draft contingency plans, but that DMDC had not fully tested the draft plans. DMDC should have responded "no" because the plans were draft documents that would not be finalized until NTS is accredited. The NTS draft contingency plans address three system-specific contingencies most likely to occur: power outages, communications failures (land line and satellite), and hardware and software failures. Additionally, the draft plans include three site-specific contingencies: natural disasters (for example, fire, flood, and earthquake), civil disorders, and bomb threats.

One draft plan includes a contingency for the primary server for the U.S. Forces Korea theater becoming inoperable. If that event were to occur, data would then go to the backup server in the southern part of the Korean Peninsula. If the server also becomes inoperable, a server at DMDC-West could be employed as the primary NTS server. All the servers were to be protected by uninterruptible power supplies. Another of the contingencies addressed the loss of power in an evacuation control center and no local backup source available. If that were to happen, the users processing noncombatants would revert to a manual process to complete noncombatant evacuation operations. As reported by DMDC, the draft contingency plan had not been tested. However, DMDC had executed parts of the draft plan, such as use of satellite communications and the use of the DMDC-West server as the primary server. Manual processing to complete noncombatant evacuation operations and site-specific contingencies were not practiced.

Hardware and System Software Maintenance Plans. DMDC was requested to identify if hardware and software maintenance plans were in place. ASD(C^3I) defined hardware and software maintenance plans as controls used for monitoring the installation of, and update to, hardware and software to ensure that the system functions as expected and that a historical record of changes are

maintained. DMDC responded in the matrix that NTS had hardware and system software maintenance plans in place. We confirmed that NTS had a draft hardware and system software maintenance plan. DMDC should have responded "no" because as of August 1, 2001, the plan was a draft document that would not be finalized until NTS is accredited. The NTS draft maintenance plan required that hardware be maintained and tested prior to training exercises and noncombatant evacuation operations. Hardware testing was to be performed quarterly. Commercial-off-the-shelf equipment warranties provided hardware maintenance for the system as required.

The draft maintenance plan called for NTS application software to be updated annually, or as required based on user feedback. DMDC collected feedback from the users and provided periodic software updates based on requested system characteristics or if flaws were discovered through usage.

Data Integrity Process. DMDC was requested to identify if data integrity processes were in place. ASD(C^3I) defined data integrity process as controls used to protect data from accidental or malicious alteration or destruction and used to provide assurance for users that the information met expectations about its quality and integrity. DMDC responded in the matrix that NTS had data integrity processes in place. We verified that NTS had a data integrity process. NTS used a "layered protection" concept that included multilevel password protection of NTS software that minimized unauthorized access of the operating system and information, and encryption that guaranteed integrity and confidentiality. The concept was facilitated in NTS through the use of software controls and the physical, personnel, and procedural measures.

Security Incident Response Plan. DMDC was requested to identify if a security incident response plan was in place. ASD(C^3I) defined a security incident response plan as a formal description and evaluation of risks to an information system, and a process that identified and applied countermeasures commensurate with the value of the assets protected based on a risk assessment. An incident response plan should have help capability when an adverse event in a computer system or network causes a failure of a security mechanism or when an attempted breach of those mechanisms occurs. DMDC responded in the matrix that NTS did not have a security incident response plan in place. We confirmed the response. As of August 1, 2001, DMDC had not developed a plan. However, since that time, a draft security incident response plan was developed. The draft plan provided general guidelines for the systematic response to unauthorized system intrusions associated with NTS. Additionally, the draft plan established rules and practices that facilitated an orderly and controlled evaluation and clean-up of any unauthorized intrusion associated with the NTS application.

Operations and Assessment Interest Items. DMDC was requested to identify specific operational assessment mechanisms as well as provide general comments to augment reporting efforts on the basic program management, controls, and procedures that existed as part of the operation of the system in the operations and assessment interest items section of the matrix. ASD(C^3I) did not provide definitions for reporting elements contained in the section. Information contained in the operations and assessment interest items section of the matrix included network protections, vulnerabilities, assessments, and system interfaces.

Network Protections. ASD(C^3I) requested data from DMDC on the network security functions of intrusion detection systems and firewalls.

- **Intrusion Detection System.** DMDC was requested to identify if an intrusion detection system protected the NTS was present. An intrusion detection system inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

- **Firewalls.** DMDC was requested to identify if boundary protections, such as firewalls, that protected the NTS were present. A firewall is a boundary protection system that limits access between networks to prevent intrusions from outside the network. A firewall stops external intrusions, but does not detect an attack from inside the network.

DMDC responded in the matrix that NTS was protected by an intrusion detection system and had boundary protection in place. We confirmed that NTS was protected by intrusion detection and a firewall at the DMDC-West site. NTS was a stand-alone system and not connected to a network. As a result, NTS did not include an intrusion detection system or firewalls at operation units. However, the DMDC-West intrusion detection system and firewalls protected the NTS data on the DMDC-West server and NTS Web site.

Vulnerabilities. ASD(C^3I) requested information from DMDC on the NTS compliance with the information assurance vulnerability alert process and vulnerability analysis and assessment program procedures.

Information Assurance Vulnerability Alert. DMDC was requested to identify if NTS was fully information assurance vulnerability alert compliant in both acknowledging and adhering to information assurance vulnerability alerts. An information assurance vulnerability alert is a process that incorporates identification and evaluation of new vulnerabilities, disseminates technical responses, and tracks compliance within DoD. Alerts are generated when a critical vulnerability that poses an immediate threat to DoD exists. DMDC did not provide a response in the matrix. We confirmed that the DMDC response was appropriate as of August 1, 2001, because DMDC did not have an information assurance vulnerability alert plan. However, since that time, DMDC began developing an information assurance vulnerability alert plan expected to be finalized by August 2002.

Vulnerability Analysis and Assessment Program. DMDC was requested to identify if NTS had a vulnerability analysis and assistance program assessment. According to the NTS draft SSAA, a vulnerability analysis and assessment program was a systematic examination of an information system that determined the adequacy of security measures, identified security deficiencies, provided data from which to predict the effectiveness of proposed security measures, and confirmed the adequacy of measures after implementation. DMDC did not provide a response in the matrix. We confirmed that the DMDC response was correct as of August 1, 2001. However, since that time,

DMDC proceeded with development of a vulnerability analysis and assessment program expected to be completed by August 2002.

Assessments. DMDC was requested to identify the dates for the most recent:

- red and blue team assessment
- Joint Staff integrated vulnerability assessment
- system requirements reviews
- balance survivability assessment
- integrated vulnerability assessment

DMDC provided no response in the matrix. We confirmed that the DMDC response was correct as of August 1, 2001, because the reporting elements in the section were specific assessments and technical controls that not all systems were required to perform, which included NTS.

System Interfaces. DMDC was requested to identify if NTS required a connection approval to connect to a larger backbone network. System interfaces are connections to other information systems for the purpose of transmitting or receiving data. DMDC did not provide a response in the matrix. We confirmed that the DMDC response was appropriate because NTS was a stand-alone system that had no active interface with other systems.

Conclusion

From our analysis of the data reported in the matrix for the NTS, we concluded that DMDC was following DITSCAP to certify and accredit NTS. Although 6 of 32 responses provided in the matrix were technically incorrect because the documents were in draft form, we further concluded that DMDC was making progress in achieving full information security accreditation for NTS by August 2002.

Appendix A. Audit Process

Scope

Work Performed. We verified and validated the NTS data supporting the DoD GISR Act Report. To accomplish the audit objective, we:

- reviewed Public Law 106-398, Office of Management and Budget guidance, and the DoD regulations and guidance related to the GISR Act;
- interviewed NTS personnel in DMDC who prepared the GISR Act matrix submission;
- verified the information reported on the GISR Act data collection matrix. Our verification consisted of reviewing the documentation that supported the answers DMDC provided on the GISR Act collection matrix as of August 1, 2001; and
- reviewed certification and accreditation documentation DMDC had developed subsequent to August 1, 2001.

Limitations to Audit Scope. We limited the audit scope to verification and validation of information in the NTS GISR Act collection matrix submission and certification and accreditation progress made since; we did not perform an operational review on NTS site certification and accreditation process. We did not perform that review because NTS is an inactive system until an evacuation operation or military exercise is performed in a military theater of operations. As a practical matter, we did not visit operational sites in Korea, Japan, and Europe to observe the physical security of deployed systems not in use. Additionally, we did not review the management control program because DoD recognized information assurance programs as a material weakness in its FY 2000 Statement of Assurance, which was its most recent, signed Statement of Assurance.

High-Risk Area. The General Accounting Office has identified several high-risk areas in DoD. This report provides coverage of the Information Security high-risk area.

Methodology

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Audit Type, Dates, and Standards. This program audit was performed from January through March 2002 in accordance with generally accepted government auditing standards.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Prior Coverage

No prior coverage has been conducted on NTS during the last 5 years.

Appendix B. Government Information Security Reform Act Collection Matrix Submission

We evaluated the GISR Act collection matrix that DMDC submitted as of August 2001 to ASD(C^3I). The following is a summary on the data ASD(C^3I) requested, the response from DMDC, and our audit analysis of the response for 26 of 32 fields on the data collection matrix. We did not include in the matrix below administrative information of the four fields that related to system identification and two of the fields that were not applicable. A list of acronyms is at the end of this appendix.

Accreditation Information		
Data Requested	**DMDC Response[4, 5]**	**Audit Results**
Accredited? (Date)	Blank	The DMDC goal was to accredit NTS by August 2002.
Interim Authority to Operate? (Date)	July 27, 2001	Interim authority to operate NTS was granted by the Designated Approving Authority (Director, DMDC) and was good for 1 year.
Accreditation under DITSCAP?	Yes	DMDC should have responded "no" because the NTS was not accredited as of August 1, 2001. DMDC was following DITSCAP to certify and accredit NTS, and planned for a full accreditation by August 2002.
Formal Documentation in effect? (SSAA or other certification and accreditation documentation)	Yes	DMDC should have responded "no" because the SSAA was a draft document as of August 1, 2001. DMDC documented the NTS certification and accreditation process with a draft SSAA. The draft SSAA will be formalized when the system is accredited.

[4]Some questions request a date only. If a date was provided, it can be implied that the answer was yes.

[5]Some questions were answered as Yes, No, or DITSCAP; the answers indicate if the system or network was accredited by DITSCAP, inherently, it would have these items in place

Assessment Criteria Information		
Data Requested	**DMDC Response**	**Audit Results**
Access controls in place?	Yes	The NTS used passwords and user accounts. – Users logged onto laptop computers using a three-digit code – Passwords were alphanumeric and included special characters – Web users were required to establish an account and a password The miniserver verified a laptop computer's hardware identification code prior to allowing access.
Risk Assessment and Management Plan completed?	No	DMDC had not completed the risk assessment and management plan. The NTS risk vulnerability assessment was in draft and scheduled to be completed by August 2002.
System Life-Cycle Plan exists?	Yes	DMDC should have responded "no" because the SSAA was a draft document. The draft SSAA included a basic system life-cycle plan. The life-cycle plan was to be revised as commercial-off-the-shelf technology was upgraded and new policies were instituted.
System Security Plan in place?	Yes	DMDC should have responded "no" because the SSAA was a draft document. The draft SSAA included a security plan as an appendix. – Standardized procedures were provided to users

Assessment Criteria Information (cont'd)		
Data Requested	**DMCD Response**	**Audit Results**
Proper Personnel Security measures in place? (includes assignment of duties and segregation of duties)	Yes	NTS had separate levels of users, with varying levels of access and control. – System administrators – Evacuation Control Center Officer in Charge – Registrars (operator and user) Passwords were required to be changed every 6 months.
Physical Security Controls in place?	Yes	NTS equipment was to be secured by the owner when not in use. When deployed, the systems were to be guarded by user unit personnel – Guards were to be posted at registration center entrances – Noncombatants were to be physically searched before entering registration centers
Administrative controls in place? (includes help desk and audit trail)	Yes	NTS draft SSAA required user unit administrators to ensure that all Federal, DoD, and local computer security-related standards were being enforced. Even though the draft SSAA required no specific NTS system level administrative controls, DMDC staffed a help desk during evacuation exercises.
Contingency Plans in place?	Yes	DMDC should have responded "no" because the contingency plan was a draft document. The draft contingency plan addressed three contingencies most likely to occur: power outages, communications failures, and hardware and software failures. DMDC-West was the backup site server for the U.S. Forces Korea server. – If Korea servers were down or destroyed, the information on the miniserver was to be pushed to a DMDC-West server

Assessment Criteria Information (cont'd)		
Data Requested	**DMDC Response**	**Audit Results**
Date Contingency Plans last exercised?	Blank	The draft contingency plan had not been fully exercised but pieces of the draft plan, such as the use of satellite communications, were.
Hardware and System Software Maintenance Plans in place? (includes version control testing)	Yes	DMDC should have responded "no" because the maintenance plans were draft documents. According to the draft plans, maintenance was to be verified and equipment tested prior to training exercises. – Hardware and system maintenance testing quarterly – Hardware was replaced by use of warranties (commercial off the shelf hardware) Software was updated annually, or as required based on user feedback.
Data integrity process in place? (includes virus scans SOP [standing operating procedure], system performance monitoring)	Yes	NTS data integrity process was facilitated through the use of software controls, physical, personnel, and procedural measures NTS used a layered protection concept – Multilevel password protection of system software and data – Encryption of data transitions
Security Incident Response Plan in place?	No	Security Incident Response Plan was added to the draft SSAA since the GISR Act data collection matrix submitted. – An incident reports database, kept at DMDC, was also added

Operations and Assessments Interest Items		
Data Requested	**DMDC Response**	**Audit Results**
Protected by IDS [Intrusion Detection Software]?	Yes	Because NTS was a stand-alone system, IDS was not necessary or used at field-level activities, but IDS protected the NTS information sent to DMDC Web site. Nothing in place to detect hackers. – Users could make unlimited login attempts to the laptop computers and Web site. – No database to hack until a noncombatant evacuation operation was in progress.
Boundary protection in place? (For example, firewall)	Yes	The DMDC server was behind a firewall, but NTS application was outside a firewall.
Red and Blue Team Assessment? (Date)	Blank	No red and blue team assessments were performed.
Connection Approved?	Blank	NTS was a stand-alone system and had no interface with other systems. The DMDC server could only extract data from NTS when DMDC dialed in – Data were pulled only when an exercise or an evacuation was in progress.
IAVA [Information Assurance Vulnerability Alerts] Compliant?	Blank	At the time matrix data was submitted, DMDC did not know what the IAVA process was. Since the data were submitted, DMDC had partially developed an NTS IAVA plan expected to be completed by August 2002.
VAAP [Vulnerability Analysis and Assessment Program] Complete? (Date)	Blank	The VAAP was partially completed and expected to be completed by August 2002.

Operations and Assessments Interest Items (cont'd)		
Data Requested	**DMDC Response**	**Audit Results**
Joint Staff Integrated Vulnerability Assessments Complete? (Date)	Blank	DMDC personnel indicated that they did not obtain any information on the subject.
System Requirements Reviews Complete? (Date)	Blank	According to DMDC, the reviews were not applicable because NTS was a Component-level system. – NTS had only a functional requirements document
Balance Survivability Assessment Complete? (Date)	Blank	DMDC did not obtain any information on this subject.
Integrated Vulnerability Assessment Complete? (Date)	Blank	NTS is a stand-alone system and had not integrated with any other systems.

Applicable Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
DITSCAP	Defense Information Technology Security Certification and Accreditation Process
DMDC	Defense Manpower Data Center
GISRA	Government Information Security Reform Act
IAVA	Information Assurance Vulnerability Alerts
IDS	Intrusion Detection Software
NTS	Noncombatant Evacuation Operations Tracking System
SOP	Standing Operating Procedure
SSAA	System Security Authorization Agreement
VAAP	Vulnerability Analysis and Assessment Program

Appendix C. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Director, Defense-Wide Information Assurance Program

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Auditor General, Department of the Air Force

Other Defense Organizations

Inspector General, Defense Intelligence Agency
Director, Defense Logistics Agency
Director, Defense Finance and Accounting Service
  Chief Information Officer
Director, DoD Human Resources Activity
  Director, Defense Manpower Data Center
Inspector General, Defense Information Systems Agency

Non-Defense Federal Organizations

Office of Management and Budget
General Accounting Office

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform
House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Audit Team Members

The Readiness and Logistics Support Directorate, Office of the Assistant Inspector General for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Shelton R. Young
Kimberley A. Caprio
Tilghman A. Schraden
Kathryn L. Palmer
Walter S. Bohinski
Stuart W. Josephs
Jason T. Steinhart
Susan R. Ryan
Daniel L. Messner
Sharon L. Carvalho